IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A transmitter device which transmits a content to a receiver device by driving a recording medium that stores the content and management data changed based on usage of the content, the transmitter device comprising:

storage means for storing a ~~check~~ hash value calculated on the basis of the management data;

communication means which, in authenticating of the receiver device, transmits the management data to the receiver device and receives a ~~check~~ hash value calculated on the basis of the management data and a ~~check~~ hash value calculated on the basis of management data changed based on the usage of the content from the receiver device;

determination means for determining whether the ~~check~~ hash value of the management data received by the communication means matches the ~~check~~ hash value of the management data stored in the storage means; and

updater means for updating the ~~check~~ hash value of the management data stored in the storage means to the ~~check~~ hash value of the changed management data.

Claim 2 (Currently Amended): A transmitter device according of Claim 1, wherein the storage means inhibits the writing or reading of the ~~check~~ hash value of the management data in a process other than the authentication process.

Claim 3 (Previously Presented): A transmitter device according to Claim 1, wherein the storage means is tamper resistant.

Claim 4 (Currently Amended): A method of transmitting a content to a receiver device by driving a recording medium that stores the content and management data changed based on usage of the content, the transmitting method comprising:

a step of storing a ~~check~~ hash value calculated on the basis of the management data;

in an authenticating step of the receiver device, a step of communication for transmitting the management data to the receiver device and for receiving a ~~check~~ hash value calculated on the basis of the management data and a ~~check~~ hash value calculated on the basis of management data changed based on the usage of the content from the receiver device;

in the authenticating of the receiver device, a step of determining whether the ~~check~~ hash value of the management data received in the communication step matches the ~~check~~ hash value of the management data stored in the storing step; and

a step of updating the ~~check~~ hash value of the management data stored in the storage means to the ~~check~~ hash value of the changed management data.

Claim 5 (Currently Amended): A program storage medium for storing a transmission process program for transmitting content to a receiver device by driving a recording medium that stores the content and management data changed based on usage of the content ~~t~~, the program executed by a transmitter device and comprising:

a step of storing a ~~check~~ hash value calculated on the basis of the management data;

in an authenticating step of the receiver device, a step of communication for transmitting the management data to the receiver device and for receiving a ~~check~~ hash value calculated on the basis of the management data and a ~~check~~ hash value calculated on the basis of management changed data based on the usage of the content from the receiver device;

in the authenticating of the receiver device, a step of determining whether the ~~check~~ hash value of the management data received in the communication step matches the ~~check~~ hash value of the management data stored in the storing step; and

a step of updating the ~~check~~ hash value of the management data stored in the storage means to the ~~check~~ hash value of the changed management data.

Claim 6 (Currently Amended): A receiver device for receiving a content from a transmitter device, the receiver device comprising:

communication means which, in authenticating of the transmitter device, receives from the transmitter device, a management data changed based on usage of the content and transmits a ~~check~~ hash value calculated on the basis of the management data to the transmitter device; and

encrypted value generator means for generating the ~~check~~ hash value of the management data based on the management data received by the communication means, in the authenticating of the transmitter device, said ~~check~~ hash value for detecting whether the management data has been tampered with.

Claim 7 (Currently Amended): A receiver device according to Claim 6, further comprising

random number generator means for generating a random number having a predetermined bit number, wherein the communication means transmits, to the transmitter device, the ~~check~~ hash value of the management data together with the random number generated by the random number generator means.

Claim 8 (Currently Amended): A receiver device according to Claim 6, further comprising data generator means for generating management data changed based on the usage of the content,

wherein the encrypted value generator means generates a ~~check~~ hash value generated on the basis of the changed management data, and

the communication means transmits, to the transmitter device, the ~~check~~ hash value of the management data together with the ~~check~~ hash value of the changed management data.

Claim 9 (Currently Amended): A method of receiving content from a transmitter device, comprising:

in the authenticating of the transmitter device, a step of communication for receiving, from the transmitter device, management data changed based on usage of the content and for transmitting a ~~check~~ hash value calculated on the basis of the management data to the transmitter device; and

in the authenticating of the transmitter device, a step of generating a ~~check~~ hash value of the management data based on the management data received in the communication step, said ~~check~~ hash value for detecting whether said management data has been tampered with.

Claim 10 (Currently Amended): A program storage medium for storing a reception process program for receiving content from a transmitter device, the program executed by a receiver device and comprising:

in the authenticating of the transmitter device, a step of communication for receiving, from the transmitter device, management data changed based on usage of the content and for transmitting a ~~check~~ hash value calculated on the basis of the management data to the transmitter device; and

in the authenticating of the transmitter device, a step of generating a ~~check~~ hash value of the management data based on the management data received in the communication step, said ~~check~~ hash value for detecting whether said management data has been tampered with.

Claim 11 (Currently Amended): A communication system comprising a transmitter device which transmits a content by driving a recording medium that stores the content and management data changed based on usage of the content, and a receiver device for receiving the content;

the transmitter device comprising:

storage means for storing a ~~check~~ hash value calculated on the basis of the management data;

first communication means which, in authenticating of the receiver device, transmits the management data to the receiver device and receives a ~~check~~ hash value calculated on the basis of the management data and a ~~check~~ hash value calculated on the basis of management data changed based on the usage of the content from the receiver device;

determination means for determining whether the ~~check~~ hash value of the management data received by the communication means matches the ~~check~~ hash value of the management data stored in the storage means; and

updater means for updating the ~~check~~ hash value of the management data stored in the storage means to the ~~check~~ hash value of the changed management data; and

the receiver device comprising:

second communication means which, in authenticating of the transmitter device, receives from the transmitter device, a management data changed based on

usage of the content and transmits a ~~check~~ hash value calculated on the basis of the management data to the transmitter device; and

encrypted value generator means for generating the ~~check~~ hash value of the management data based on the management data received by the communication means, in the authenticating of the transmitter device, said ~~check~~ hash value for detecting whether the management data has been tampered with.

Claims 12-25 (Canceled).